Remarks/Arguments

Claims 1 and 36 to 47 are now pending and under examination in the application and are subject to discussion. Claims 1, 36 and 41 are amended. Claims 2 to 13, 48 and 49 are cancelled. Claims 14-35 and 50-57 were previously withdrawn. No new subject matter is added to the application through the present amendments.

Claim rejection under 35 U.S.C. § 103(a)

Over Shimizu et al. (US 6,085,323) in view of Al-Salqan (US 6,775,382 B1) and further in view of Schneier et al. (US 7,362,862 B2)

Claims 1 is rejected under 35 U.S.C. § 103(a). The Applicant amends claim 1 and now believes claim 1 to be unobvious in view of the cited references.

Claim 1 is amended to specify in more detail the different communications and processes performed by the different components of the system (sender FIPS, sender SIPS, receiver FIPS and receiver SIPS) and precisely identifying the components performing the different communications and processes.

Furthermore, claim 1 now recites a limitation regarding the coordination of a common second encryption key between the sender and the receiver that permits, following that common encryption key coordination, to the sender and the receiver to exchange sensitive data in a more secured manner than the prior art allows. Claim 1 now recites:

> *"wherein the sender and the receiver can initiate a pairing process over said generally unsecured transmission link during which pairing process the sender SIPS and the receiver SIPS exchange signals to establish the use of a common second encryption key without communicating said second encryption key over said generally unsecured transmission link."*

Support for this amendment can be found at least in paragraphs 116 to 120.

The Applicant believes that the foregoing amendment overcomes the Office Action's rejections in view of any of the above references or any Applicant's known references. The

above amendment clearly states that a coordination of the SIPSs information can be performed and association of a common second encryption key associated with the receiver (for the sender SIPS) and with the sender (for the receiver SIPS) without the second encryption key being communicated over an unsecured transmission link (e.g., the Internet), or even to a FIPS to which a SIPS may be connected or any other unsecured transmission link.

Shimizu does not teach this limitation. Shimizu teaches having a plurality of potential receivers to select from (see Figure 12) but does not teach how the different receivers are associated with encryption keys and furthermore how the above described coordination of the encryption keys is performed.

For its part, Al-Salqan provides a system wherein a private key is communicated to a recipient over the Internet following a private key request and a successful identification. Therefore, Al-Salqan does not refer at all to the problem of security resolved by the present invention by preventing communication of encryption keys over an unsecured communication link.

The field of teaching of Schneier is, for its part, very distinct from security in communications. Furthermore, the teaching of Schneier provides no clue on ways of performing such an encryption key coordination between two recipients without communication of said encryption key.

Accordingly, it is the Applicant's opinion that claim 1 is now in condition for allowance. Withdrawal of the rejection of claim 1 is therefore respectfully requested.

Referring to claim 36, it is amended to integrate a limitation similar to the above discussed claim 1 limitation. Claim 36 now recites:

> *"wherein said correspondent key is established with a correspondent system prior to performing said information processing method without having communicated said identified correspondent key outside said SIPS."*

Support for this amendment can be found at least in paragraphs 116 to 120.

Amended claim 36 clearly recites a limitation for the coordination of an encryption key between two recipients without communicating said encryption key over an unsecured communication link.

In view of the arguments relating to claim 1 arguments and the nature of the amendment of claim 36, it is the Applicant's opinion the claim 36 is now in condition for allowance. Withdrawal of the rejection of claim 36 is therefore respectfully requested.

Referring to claim 41, it is herein amended to integrate a limitation similar to the amendments made to claim 36 and to claim 1. Claim 41 now recites:

> *"wherein said correspondent key is established with a system which has generated said integrated secured sensitive data prior to performing said information processing method without having communicated said identified correspondent key outside said SIPS."*

Support for this amendment can be found at least in paragraphs 116 to 120.

Claim 41 amended clearly recites a limitation for the coordination of an encryption key between two recipients without communicating said encryption key over an unsecured communication link.

In view of the arguments relating to claim 1 and claim 36 and the nature of the amendment of claim 41, it is the Applicant's opinion the claim 41 is now in condition for allowance. Withdrawal of the rejection of claim 41 is therefore respectfully requested.

The Applicant submits that all other claims rejected or otherwise allowable herein not discussed, are dependent upon claim 1, claim 36 or claim 41 and thus should be found allowable.

It is submitted therefore that claims 1 and 36 to 47 are in condition for allowance.

Reconsideration of claim rejections is respectfully requested and allowance of claims 1 and 36 to 47 at an early date is solicited.

In the event that there are any questions concerning the Response to Office Action or the application in general, the Examiner is respectfully urged to telephone the undersigned so that prosecution of this application may be expedited.

Respectfully submitted,

Denis Bisson

By:

/C. Marc Benoît/
C. Marc Benoît
(Reg. 50,200)
Agent of Record
Benoît & Co.
Tel: (450) 646-9997